UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/905,533	07/14/2001	Myles Jordan	655/62436	3486

7590 05/04/2005

Richard F. Jaworski
Cooper & Dunham LLP
1185 Avenue of the Americas
New York, NY 10036

EXAMINER	
SCHUBERT, KEVIN R	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 05/04/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/905,533	JORDAN, MYLES	
	Examiner	Art Unit	
	Kevin Schubert	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *14 April 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-18* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-18* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *14 April 2005* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claims 1-18 have been considered.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-18 are rejected under 35 U.S.C. 102(e) as being unpatentable by Nachenberg, U.S. Patent No. 6,357,008.

As per claims 1,7,9, and 17, the applicant discloses the following method which is anticipated by Nachenberg:

a) emulating computer executable code in a subject file (Col 7, lines 9-12);

b) flagging a memory area that is read during emulation of a first instruction in the computer executable code (Col 9, lines 5-10);

c) detecting a modification to the flagged memory area during emulation of a second instruction in the computer executable code (Col 9, lines 5-10);

The applicant should note that claim 9 also claims a processor which is disclosed by Nachenberg in the Description of the Preferred Embodiments (Col 6, lines 22-24).

As per claims 2,8,10, and 18, the applicant discloses the following method which is anticipated by Nachenberg:

a) emulating computer executable code in a subject file (Col 7, lines 9-12);

b) maintaining a list of memory regions that have been read and then modified during the emulation (Col 9, lines 11-14);

c) determining whether a memory area is read during emulation of a first instruction in the computer executable code and whether the memory area is modified during emulation of a second instruction in the computer executable code (Col 9, lines 5-10);

d) updating the list of memory regions to include the modified memory area (Col 9, lines 11-14);

e) triggering a viral detection alarm, if one of the listed memory regions is larger than a predetermined size (Col 8, lines 1-7);

The applicant should note that claim 10 also claims a processor which is disclosed by Nachenberg in the Description of the Preferred Embodiments (Col 6, lines 22-24).

As per claims 3 and 13, the applicant discloses the method of claims 2 and 12, respectively, which are anticipated by Nachenberg (see above) with the following limitation which is also anticipated by Nachenberg:

Wherein the emulation is performed on an instruction-by-instruction basis (Col 7, lines 55-67);

As per claims 4 and 14, the applicant discloses the method of claims 2 and 12, respectively, which are anticipated by Nachenberg (see above) with the following limitations which are also anticipated by Nachenberg:

a) determining whether a selected one of the listed memory regions overlaps the modified memory area (Figure 4B);

b) updating the selected memory region to encompass the modified memory area (Col 9, lines 11-14);

The application should note that step 420 of Figure 4B is the determination step as to whether the modified memory area has already been noted. This determination step identifies whether the modified memory area has already been noted in whole or in part, so if there is an overlap, this step picks that up.

As per claims 5 and 15, the applicant discloses the method of claims 2 and 12, respectively, which are anticipated by Nachenberg (see above) with the following limitations which are also anticipated by Nachenberg:

a) determining whether a selected one of the listed memory regions is contiguous with the modified memory area (Col 18, lines 5-7; Figure 4B; Claim 16);

b) updating the selected memory region to encompass the modified memory area (Col 9, lines 11-14);

Pertaining to part a), the applicant should note that Nachenberg leaves the determination of the virus region in step 420 of Figure 4 open (Col 18, lines 5-7). This means that Nachenberg allows for a variety of methods to identify the virus region. Nachenberg also discusses in claim 16 that identifying contiguous sections of modified bytes in memory is an easy way to discern whether the viral body has decrypted. Thus, a method to monitor whether a selected region is contiguous with a modified region is one of several ways to identify a virus region and is implicitly covered in the determination of the virus region step of Figure 4.

As per claims 6 and 16, the applicant discloses the method of claims 2 and 12, respectively, which are anticipated by Nachenberg (see above) with the following limitations which are also anticipated by Nachenberg:

a) determining whether the modified memory area overlaps the listed memory regions (Figure 4B);

b) adding the modified memory area as a new memory region to the list of memory regions, if the modified memory area does not overlap any of the listed memory regions (Col 9, lines 11-14);

The application should note that step 420 of Figure 4B is the determination step as to whether the modified memory area has already been noted. This determination step would identify whether the modified memory area has already been noted in whole or in part, so if there were an overlap, this step would pick that up.

As per claim 11, the applicant discloses the following apparatus for detecting decryption of encrypted viral code with the following limitations:

a) a code emulator, wherein the code emulator emulates computer executable code in a subject file, and outputs memory access information corresponding to the emulated computer executable code (Col 7, lines 9-12; Col 7, lines 17-21);

b) a memory monitor, wherein the memory monitor monitors the memory access information output by the code emulator, flags a memory area that is read during the emulation of a first instruction in the computer executable code, and detects a modification to the flagged memory area during emulation of a second instruction in the computer executable code (Col 9, lines 5-14);

As per claim 12, the applicant discloses the following apparatus for detecting decryption of encrypted viral code with the following limitations:

a) a code emulator, wherein the code emulator emulates computer executable code in a subject file, and outputs memory access information corresponding to the emulated computer executable code (Col 7, lines 9-12; Col 7, lines 17-21);

b) a memory monitor, wherein the memory monitor monitors the memory access information output by the code emulator, maintains a list of memory regions that have been read and modified during emulation, determines whether a memory area is read during emulation of a first instruction in the computer executable code and whether the memory area is modified during emulation of a second instruction in the computer executable code, updates the list of memory regions to include the modified memory area, and triggers a viral detection alarm, if one of the listed memory regions is larger than a predetermined size (Col 9, lines 5-14; Col 8, lines 1-7).

Response to Arguments

The applicant's remarks, filed 4/14/05, with regard to the new drawings have been fully considered. The new drawings are accepted.

Applicant's arguments with regard to claim 1 have been fully considered but they are not persuasive. The applicant argues that the primary reference, Nachenberg, merely detects a modification to the instruction and not the virtual memory space. The examiner disagrees. One of the suspicious operations that is evaluated is the "modification of memory allocation" (Col 9, lines 54-55).

Applicant's arguments with regard to claim 2 fail to comply with 37 CFR 1.111(b) because they amount to a general allegation that the claims define a patentable invention without specifically pointing out how the language of the claims patentably distinguishes them from the references. The applicant gives no reasons for how the applicant's claimed invention is different from the primary reference, Nachenberg. The applicant merely says the claimed invention is patentably distinct and restates the limitations of claim 2.

Conclusion

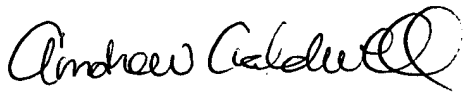
THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kevin Schubert whose telephone number is (571) 272-4239. The examiner can normally be reached on M-F 8:00-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on (571) 272-3868. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



ANDREW CALDWELL
SUPERVISORY PATENT EXAMINER